

National Cyber Alert System

Cyber Security Bulletin SB09-236

[Archive](#)

Vulnerability Summary for the Week of August 17, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
2fly -- gift_delivery_system	SQL injection vulnerability in 2fly_gift.php in 2FLY Gift Delivery System 6.0 allows remote attackers to execute arbitrary SQL commands via the gameid parameter in a content action.	2009-08-21	7.5	CVE-2009-2915 SECUNIA MISC	
2kgames -- vietcong2	Format string vulnerability in the CNS_AddTxt function in logs.dll in 2K Games Vietcong 2 1.10 and earlier might allow remote attackers to execute arbitrary code via format string specifiers in the nickname.	2009-08-21	10.0	CVE-2009-2916 XF SECUNIA OSVDB MISC	
accellion -- file_transfer_appliance_fta	courier/1000@/api_error_email.html (aka "error reporting page") in Accellion File Transfer Appliance FTA_7_0_178, and possibly other versions before FTA_7_0_189, allows remote attackers to send spam e-mail via modified description and client_email parameters.	2009-08-19	7.8	CVE-2008-7012 MISC XF SECTRACK BID SECUNIA OSVDB	
acer -- lunchapp.aplunch	The Acer LunchApp (aka AcerCtrls.APlunch) ActiveX control in acerctrl.ocx allows remote attackers to execute arbitrary commands via the Run method, a different vulnerability than CVE-2006-6121.	2009-08-19	9.3	CVE-2009-2627 CERT-VN VUPEN	

adium -- adium pidgin -- pidgin	The msn_slplink_process_msg function in libpurple/protocols/msn/slplink.c in libpurple, as used in Pidgin (formerly Gaim) before 2.5.9 and Adium 1.3.5 and earlier, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by sending multiple crafted SLP (aka MSNSLP) messages to trigger an overwrite of an arbitrary memory location. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2009-1376.	2009-08-21	10.0	CVE-2009-2694 CONFIRM
aj_square -- aj_article	AJ Square AJ Article allows remote attackers to bypass authentication and access administrator functionality via a direct request to (1) user.php, (2) articles.php, (3) articlesuspend.php, (4) site.php, (5) statistics.php, (6) mail.php, (7) category.php, (8) subcategory.php, (9) changepassword.php, (10) polling.php, and (11) logo.php in admin/.	2009-08-24	7.5	CVE-2008-7051 VUPEN BID MILWoRM
artis.imag -- basilic	Multiple SQL injection vulnerabilities in Basilic 1.5.13 allow remote attackers to execute arbitrary SQL commands via the idAuthor parameter to (1) index.php and possibly (2) allpubs.php in publications/.	2009-08-20	7.5	CVE-2009-2881 XF VUPEN MILWoRM
aruba_networks -- aruba_mobility_controller arubanetworks -- arubaos	Aruba Mobility Controller running ArubaOS 3.3.1.16, and possibly other versions, installs the same default X.509 certificate for all installations, which allows remote attackers to bypass authentication. NOTE: this is only a vulnerability when the administrator does not follow recommendations in the product's security documentation.	2009-08-21	10.0	CVE-2008-7023 BID BUGTRAQ BUGTRAQ OSVDB
aves -- rpg_board	RPG.Board 0.8 Beta2 and earlier allows remote attackers to bypass authentication and gain privileges by setting the keep4u cookie to a certain value.	2009-08-21	7.5	CVE-2008-7028 XF BID MILWoRM
chilkatsoft -- chilkat_imap_activex_control	Insecure method vulnerability in ChilkatMail_v7_9.dll in the Chilkat Software IMAP ActiveX control (ChilkatMail2.ChilkatMailMan2.1) allows remote attackers to execute arbitrary programs via the LoadXmlEmail method.	2009-08-21	9.3	CVE-2008-7022 XF MILWoRM
cisco -- firewall_services_module	The Cisco Firewall Services Module (FWSM) 2.x, 3.1 before 3.1(16), 3.2 before 3.2(13), and 4.0 before 4.0(6) for Cisco Catalyst 6500 switches and Cisco 7600 routers allows remote attackers to cause a denial of service (traffic-handling outage) via a series of malformed ICMP messages.	2009-08-21	7.8	CVE-2009-0638 CISCO
clone2009 -- ebay_clone	Multiple SQL injection vulnerabilities in Ebay Clone 2009 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to product_desc.php, and the cid parameter to (2) showcategory.php and (3) gallery.php.	2009-08-20	7.5	CVE-2009-2894 XF SECUNIA MISC OSVDB OSVDB OSVDB
cmsbright -- cmsbright	SQL injection vulnerability in public/page.php in Websens CMSbright allows remote attackers to execute arbitrary SQL commands via the id_rub_page	2009-08-19	7.5	CVE-2008-6991 BID MILWoRM

	parameter.			SECUNIA OSVDB
creative_mind -- creator_cms	Unrestricted file upload vulnerability in the file manager in Creative Mind Creator CMS 5.0 allows remote attackers to execute arbitrary code via unknown vectors.	2009-08-19	7.5	CVE-2008-7001 XF MILWoRM
devalcms -- devalcms	modules/tool/hitcounter.php in devalcms 1.4a allows remote attackers to execute arbitrary PHP code via the HTTP Referer header with a target file specified in the gv_folder_data parameter, as demonstrated by modifying modules/tool/url2header.php.	2009-08-19	7.5	CVE-2008-6983 XF BID OSVDB
digitalspinners -- ds_cms	SQL injection vulnerability in DetailFile.php in DigitalSpinners DS CMS 1.0 allows remote attackers to execute arbitrary SQL commands via the nFileDialog parameter.	2009-08-21	7.5	CVE-2009-2927 XF MILWoRM
djcalendar -- djcalendar	Directory traversal vulnerability in DJcalendar.cgi in DJCalendar allows remote attackers to read arbitrary files via a .. (dot dot) in the TEMPLATE parameter.	2009-08-21	7.8	CVE-2009-2925 XF MILWoRM
elog -- elog	Buffer overflow in Electronic Logbook (ELOG) before 2.7.1 has unknown impact and attack vectors, possibly related to elog.c.	2009-08-19	10.0	CVE-2008-7004 XF VUPEN
esqlanelapse -- esqlanelapse	Esqlanelapse 2.6.1 and 2.6.2 allows remote attackers to bypass authentication and gain privileges via modified (1) enombre and (2) euri cookies.	2009-08-21	7.5	CVE-2008-7019 XF BID MILWoRM
ezonescripts -- dating_website_script	Unrestricted file upload vulnerability in eZoneScripts Dating Website script allows remote attackers to execute arbitrary code via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-19	7.5	CVE-2008-6987 XF BID
ezphotogallery -- ezphotogallery	SQL injection vulnerability in gallery.php in Easy Photo Gallery (aka Ezphotogallery) 2.1 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-08-19	7.5	CVE-2008-6989 BUGTRAQ OSVDB MILWoRM SECUNIA
ezphotogallery -- ezphotogallery	SQL injection vulnerability in gallery.php in Easy Photo Gallery (aka Ezphotogallery) 2.1 allows remote attackers to execute arbitrary SQL commands via the password parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-19	7.5	CVE-2008-6990 OSVDB SECUNIA
galore -- com_simpleshop	SQL injection vulnerability in the Simple Shop Galore (com_simpleshop) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the section parameter in a section action to index.php, a different vulnerability than CVE-2008-2568. NOTE: this issue was disclosed by an unreliable researcher, so the details might be incorrect.	2009-08-24	7.5	CVE-2008-7033 XF BID BUGTRAQ OSVDB
	stack based buffer overflow in the SaveAs feature			CVE-2008-6994 XF

google -- chrome	Stack-based buffer overflow in the SaveAs feature (SaveFileAsWithFilter function) in win_util.cc in Google Chrome 0.2.149.27 allows user-assisted remote attackers to execute arbitrary code via a web page with a long TITLE element, which triggers the overflow when the user saves the page and a long filename is generated.	2009-08-19	9.3	BID BUGTRAQ MILWORM MISC CONFIRM SECTRACK MISC OSVDB CONFIRM
google -- chrome	Stack-based buffer overflow in chrome/common/gfx/url_elider.cc in Google Chrome 0.2.149.27 and other versions before 0.2.149.29 might allow user-assisted remote attackers to execute arbitrary code via a link target (href attribute) with a large number of path elements, which triggers the overflow when the status bar is updated after the user hovers over the link.	2009-08-19	9.3	CVE-2008-6998 CONFIRM
greensql -- greensql_firewall	GreenSQL Firewall (greensql-fw), possibly before 0.9.2 or 0.9.4, allows remote attackers to bypass the SQL injection protection mechanism via a WHERE clause containing an expression such as "x=y=z", which is successfully parsed by MySQL.	2009-08-19	7.5	CVE-2008-6992 MISC MISC
imtoo -- mpeg_encoder	Stack-based buffer overflow in ImTOO MPEG Encoder 3.1.53 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted string in a (1) .cue or (2) .m3u playlist file.	2009-08-21	9.3	CVE-2009-2917 MILWORM
joshua_oliver -- really_simple_cms	Directory traversal vulnerability in plugings/pagecontent.php in Really Simple CMS (RSCMS) 0.3a allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the PT parameter.	2009-08-17	7.5	CVE-2009-2792 XF MILWORM
kde -- kmplayer	Buffer overflow in KMplayer 2.9.4.1433 and earlier allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a long string in a subtitle (.srt) playlist file. NOTE: some of these details are obtained from third party information.	2009-08-20	9.3	CVE-2009-2896 XF VUPEN BID MILWORM
libra_file_manager -- php_filemanager	Libra File Manager 1.18 and earlier allows remote attackers to bypass authentication and gain privileges by setting the user and pass cookies to 1.	2009-08-21	7.5	CVE-2008-7027 BID MILWORM
linux -- kernel linux -- kernel	The Linux kernel 2.6.0 through 2.6.30.4, and 2.4.4 through 2.4.37.4, does not initialize all function pointers for socket operations in proto_ops structures, which allows local users to trigger a NULL pointer dereference and gain privileges by using mmap to map page zero, placing arbitrary code on this page, and then invoking an unavailable operation, as demonstrated by the sendpage operation (sock_sendpage function) on a PF_PPPOX socket.	2009-08-14	7.2	CVE-2009-2692 VUPEN
linux -- kernel linux -- kernel	The init_posix_timers function in kernel/posix-timers.c in the Linux kernel before 2.6.31-rc6 allows local users to cause a denial of service (OOPS) or possibly gain privileges via a CLOCK_MONOTONIC_RAW clock_nanosleep call that triggers a NULL pointer dereference.	2009-08-14	7.2	CVE-2009-2767 MLIST MLIST
	cfg80211 in net/wireless/scan.c in the Linux kernel			

linux -- kernel linux -- kernel	2.6.30-rc1 and other versions before 2.6.31-rc6 allows remote attackers to cause a denial of service (crash) via a sequence of beacon frames in which one frame omits an SSID Information Element (IE) and the subsequent frame contains an SSID IE, which triggers a NULL pointer dereference in the cmp_ies function. NOTE: a potential weakness in the is_mesh function was also addressed, but the relevant condition did not exist in the code, so it is not a vulnerability.	2009-08-18	7.8	CVE-2009-2844 MLIST MLIST MISC
linux -- kernel linux -- kernel	The eisa_eeprom_read function in the parisc isa-eeprom component (drivers/parisc/eisa_eeprom.c) in the Linux kernel before 2.6.31-rc6 allows local users to access restricted memory via a negative ppos argument, which bypasses a check that assumes that ppos is positive and causes an out-of-bounds read in the readb function.	2009-08-18	7.8	CVE-2009-2846 MLIST MLIST
minb -- minb_is_not_a_blog	include/modules/top/1-random_quote.php in Minb Is Not a Blog (minb) 0.1.0 allows remote attackers to execute arbitrary PHP code via the quotes_to_edit parameter. NOTE: this issue has been reported as an unrestricted file upload by some sources, but that is a potential consequence of code execution.	2009-08-19	7.5	CVE-2008-7005 XF BID BUGTRAQ MILWoRM OSVDB
mobilelib -- mobilelib_gold	Multiple SQL injection vulnerabilities in Mobilelib GOLD 3 allow remote attackers to execute arbitrary SQL commands via the (1) adminName parameter to cp/auth.php, (2) cid parameter to artcat.php, and (3) catid parameter to show.php.	2009-08-17	7.5	CVE-2009-2788 BID MILWoRM
mocdesigns -- php_news	Multiple SQL injection vulnerabilities in login.php in MOC Designs PHP News 1.1 allow remote attackers to execute arbitrary SQL commands via the (1) newsuser parameter (User field) and (2) newspassword parameter (Password field).	2009-08-21	7.5	CVE-2009-2921 XF VUPEN MILWoRM
nasa_goddard_space_flight_center -- common_data_format	Multiple buffer overflows in NASA Common Data Format (CDF) allow context-dependent attackers to execute arbitrary code, as demonstrated using (1) an array index error in the ReadAEDRList64 function, and other errors in the (2) SearchForRecord_r_64, (3) LastRecord64, (4) CDFsel64, and other unspecified functions.	2009-08-18	9.3	CVE-2009-2850 CONFIRM
natterchat -- natterchat	Multiple SQL injection vulnerabilities in login.asp in NatterChat 1.1 and 1.12 allow remote attackers to execute arbitrary SQL commands via the (1) txtUsername parameter (aka Username) and (2) txtPassword parameter (aka Password) in a form generated by home.asp. NOTE: due to lack of details, it is not clear whether this is related to CVE-2004-2206.	2009-08-24	7.5	CVE-2008-7049 XF BID MILWoRM MILWoRM
permis -- com_groups	SQL injection vulnerability in the Permis (com_groups) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a list action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-17	7.5	CVE-2009-2789 XF BID
	PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions,			

php -- php	which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.	2009-08-19	7.2	CVE-2008-7002 BID MISC
php-paid4mail -- php-paid4mail	SQL injection vulnerability in paidbanner.php in PHP Paid 4 Mail Script allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2009-08-14	7.5	CVE-2009-2774 MILWoRM SECUNIA
phpadultsite -- phpadultsite_cms	SQL injection vulnerability in as_archives.php in phpAdultSite CMS, possibly 2.3.2, allows remote attackers to execute arbitrary SQL commands via the results_per_page parameter to index.php. NOTE: some of these details are obtained from third party information.	2009-08-19	7.5	CVE-2008-6980 XF BUGTRAQ MISC SECUNIA OSVDB
phpauction -- phpauction	PHP remote file inclusion vulnerability in index.php in PHPAuction 3.2 allows remote attackers to execute arbitrary PHP code via a URL in the lan parameter. NOTE: this might be related to CVE-2005-2255.1.	2009-08-19	7.5	CVE-2008-7000 XF MISC
phpcompet.free -- php_competition_system	Multiple SQL injection vulnerabilities in PHP Competition System BETA 0.84 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) day parameter to show_matchs.php and (2) pageno parameter to persons.php.	2009-08-21	7.5	CVE-2009-2926 XF MILWoRM
phpscriptsnow -- world's_tallest_buildings	SQL injection vulnerability in bios.php in PHP Scripts Now World's Tallest Buildings allows remote attackers to execute arbitrary SQL commands via the rank parameter.	2009-08-20	7.5	CVE-2009-2885 XF OSVDB SECUNIA MISC
phpscriptsnow -- president_bios	SQL injection vulnerability in bios.php in PHP Scripts Now President Bios allows remote attackers to execute arbitrary SQL commands via the rank parameter.	2009-08-20	7.5	CVE-2009-2886 XF SECUNIA MISC
phpscriptsnow -- hangman	SQL injection vulnerability in index.php in PHP Scripts Now Hangman allows remote attackers to execute arbitrary SQL commands via the n parameter.	2009-08-20	7.5	CVE-2009-2888 XF OSVDB SECUNIA MISC
phpscriptsnow -- riddles	SQL injection vulnerability in list.php in PHP Scripts Now Riddles allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2009-08-20	7.5	CVE-2009-2891 XF OSVDB SECUNIA MISC
phpsugar -- ultimate_regnow_affiliate	SQL injection vulnerability in rss.php in Ultimate Regnow Affiliate (URA) 3.0 allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-08-20	7.5	CVE-2009-2895 MILWoRM
phnxension -- phpx -- guestbook	Free PHP VX Guestbook 1.06 allows remote attackers to bypass authentication and gain administrative	2009-08-		CVE-2008-7007 XF BID

phpversion -- php_vx_guesswork	access by setting the (1) admin_name and (2) admin_pass cookie values to 1.	19	7.5	BID MILWORM SECUNIA OSVDB
piwigo -- piwigo	SQL injection vulnerability in comments.php in Piwigo before 2.0.3 allows remote attackers to execute arbitrary SQL commands via the items_number parameter.	2009-08-21	7.5	CVE-2009-2933 MISC BUGTRAQ SECUNIA
pixaria -- pixaria_gallery	Absolute path traversal vulnerability in pixaria.image.php in Pixaria Gallery 2.0.0 through 2.3.5 allows remote attackers to read arbitrary files via a base64-encoded file parameter.	2009-08-21	7.8	CVE-2009-2922 XF BID CONFIRM MILWoRM
programmedintegration -- pipl	Multiple stack-based buffer overflows in xaudio.dll in Programmed Integration PIPL 2.5.0 and 2.5.0D allow remote attackers to execute arbitrary code via a long string in a (1) .pls or (2) .pl playlist file.	2009-08-21	9.3	CVE-2009-2934 XF MILWORM SECUNIA OSVDB
reputation -- reputation	SQL injection vulnerability in reputation.php in the Reputation plugin 2.2.4, 2.2.3, 2.0.4, and earlier for PunBB allows remote attackers to execute arbitrary SQL commands via the poster parameter.	2009-08-17	7.5	CVE-2009-2786 XF MILWoRM SECUNIA OSVDB
scripteen -- free_image_hosting_script	Multiple SQL injection vulnerabilities in header.php in Scripteen Free Image Hosting Script 2.3 allow remote attackers to execute arbitrary SQL commands via a (1) cookid or (2) cookgid cookie.	2009-08-20	7.5	CVE-2009-2892 CONFIRM
shop-o2o -- php_paid_4_mail_script	PHP remote file inclusion vulnerability in home.php in PHP Paid 4 Mail Script allows remote attackers to execute arbitrary PHP code via a URL in the page parameter.	2009-08-14	7.5	CVE-2009-2773 XF MILWoRM SECUNIA OSVDB
siemens -- gigaset_wlan_camera	Siemens Gigaset WLAN Camera 1.27 has an insecure default password, which allows remote attackers to conduct unauthorized activities. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-19	10.0	CVE-2008-6993 BID
site2nite -- real_estate_web	Multiple SQL injection vulnerabilities in Site2Nite Real Estate Web allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password field to an unspecified component, possibly agentlist.asp. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.	2009-08-24	7.5	CVE-2008-7030 XF BID BUGTRAQ OSVDB
skalinks -- exchange_script	Skalfa Software SkaLinks Exchange Script 1.5 allows remote attackers to add new administrators and gain privileges via a direct request to admin/register.php.	2009-08-19	10.0	CVE-2008-7010 XF BID MILWoRM MISC
	Directory traversal vulnerability in p.php in			CVE-2009-2931 BUGTRAQ

slideshowpro -- director	SlideShowPro Director 1.1 through 1.3.8 allows remote attackers to read arbitrary files via directory traversal sequences in the a parameter.	2009-08-21	7.8	BUGTRAQ OSVDB MISC CONFIRM SECUNIA
snom -- snom_300 snom -- snom_320 snom -- snom_360 snom -- snom_370	The web interface on the snom VoIP phones snom 300, snom 320, snom 360, snom 370, and snom 820 with firmware 6.5 before 6.5.20, 7.1 before 7.1.39, and 7.3 before 7.3.14 allows remote attackers to bypass authentication, and reconfigure the phone or make arbitrary use of the phone, via a (1) http or (2) https request with 127.0.0.1 in the Host header.	2009-08-14	10.0	CVE-2009-1048 XF BUGTRAQ MISC SECUNIA
softbiz -- dating_script	SQL injection vulnerability in cat_products.php in SoftBiz Dating Script allows remote attackers to execute arbitrary SQL commands via the cid parameter. NOTE: this might overlap CVE-2006-32714.	2009-08-17	7.5	CVE-2009-2790 XF BID MISC
tgs-cms -- tgs_content_management	Multiple SQL injection vulnerabilities in TGS Content Management 0.x allow remote attackers to execute arbitrary SQL commands via the (1) tgs_language_id, (2) tpl_dir, (3) referer, (4) user-agent, (5) site, (6) option, (7) db_optimization, (8) owner, (9) admin_email, (10) default_language, and (11) db_host parameters to cms/index.php; and the (12) cmd, (13) s_dir, (14) minutes, (15) s_mask, (16) test3_mp, (17) test15_file1, (18) submit, (19) brute_method, (20) ftp_server_port, (21) userfile14, (22) subj, (23) mysql_l, (24) action, and (25) userfile1 parameters to cms/frontpage_ception.php. NOTE: some of these parameters may be applicable only in nonstandard versions of the product, and cms/frontpage_ception.php may be cms/frontpage_caption.php in all released versions.	2009-08-21	7.5	CVE-2009-2929 XF MILWORM
the-rat-cms -- the-rat-cms	Multiple SQL injection vulnerabilities in login.php in The Rat CMS Alpha 2 allow remote attackers to execute arbitrary SQL commands via the (1) user_id and (2) password parameter.	2009-08-19	7.5	CVE-2008-7003 XF BID MILWORM
tikiwiki -- tikiwiki	TikiWiki 1.6.1 allows remote attackers to bypass authentication by entering a valid username with an arbitrary password, possibly related to the Internet Explorer "Remember Me" feature. NOTE: some of these details are obtained from third party information.	2009-08-24	7.5	CVE-2003-1574 BID CONFIRM
videosbroadcastyourself -- videos_broadcast_yourself	Multiple SQL injection vulnerabilities in Videos Broadcast Yourself 2 allow remote attackers to execute arbitrary SQL commands via the (1) UploadID parameter to videoint.php, and possibly the (2) cat_id parameter to catvideo.php and (3) uid parameter to cviewchannels.php.	2009-08-21	7.5	CVE-2009-2924 MILWORM
webdynamite -- projectbutler	PHP remote file inclusion vulnerability in pda_projects.php in WebDynamite ProjectButler 1.5.0 allows remote attackers to execute arbitrary PHP code via a URL in the offset parameter.	2009-08-17	7.5	CVE-2009-2791 BID MILWORM
wordpress -- wordpress	Wordpress before 2.8.3 allows remote attackers to gain privileges via a direct request to (1) admin-footer.php, (2) edit-category-form.php, (3) edit-form-advanced.php, (4) edit-form-comment.php, (5) edit-	2009-08-10	10.0	CVE-2009-2853

	link-category-form.php, (6) edit-link-form.php, (7) edit-page-form.php, and (8) edit-tag-form.php in wp-admin/.	10		CONFIRM
Back to top				
Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Unrestricted file upload vulnerability in usercp.php in AlilG Application AliBoard Beta allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as an avatar, then accessing it via a direct request to the file in uploads/avatars/.	2009-08-24	6.5	CVE-2008-7029 XF BID BUGTRAQ OSVDB
adobe -- coldfusion	Multiple cross-site scripting (XSS) vulnerabilities in Adobe ColdFusion Server 8.0.1, 8, and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the startRow parameter to administrator/logviewer/searchlog.cfm, or the query string to (2) wizards/common/_logintowizard.cfm, (3) wizards/common/_authenticatewizarduser.cfm, or (4) administrator/enter.cfm.	2009-08-18	4.3	CVE-2009-1872 CONFIRM
adobe -- jrun	Directory traversal vulnerability in logging/logviewer.jsp in the Management Console in Adobe JRun Application Server 4 Updater 7 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the logfile parameter.	2009-08-18	4.0	CVE-2009-1873 CONFIRM
adobe -- jrun	Multiple cross-site scripting (XSS) vulnerabilities in the Management Console in Adobe JRun 4.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-08-18	4.3	CVE-2009-1874 CONFIRM
adobe -- coldfusion	Multiple cross-site scripting (XSS) vulnerabilities in Adobe ColdFusion 8.0.1 and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2009-1877.	2009-08-18	4.3	CVE-2009-1875 CONFIRM
adobe -- coldfusion	Adobe ColdFusion 8.0.1 and earlier might allow attackers to obtain sensitive information via unspecified vectors, related to a "double-encoded null character vulnerability."	2009-08-18	5.0	CVE-2009-1876 CONFIRM
adobe -- coldfusion	Cross-site scripting (XSS) vulnerability in Adobe ColdFusion 8.0.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2009-1875.	2009-08-18	4.3	CVE-2009-1877 CONFIRM
adobe -- coldfusion	Session fixation vulnerability in Adobe ColdFusion 8.0.1 and earlier allows remote attackers to hijack web sessions via unspecified vectors.	2009-08-18	6.8	CVE-2009-1878 CONFIRM
arabless -- saphlesson	SQL injection vulnerability in admin/login.php in SaphpLesson 4.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the cp_username parameter, related to an error in the CleanVar function in includes/functions.php.	2009-08-20	6.8	CVE-2009-2883 XF BID MILWORM
				CVE-2008-7024

arzdev -- gemini_lite arzdev -- gemini_portal	admin.php in Arz Development The Gemini Portal 4.7 and earlier allows remote attackers to bypass authentication and gain administrator privileges by setting the user cookie to "admin" and setting the name parameter to "users."	2009-08-21	6.8	/U24 XF BID BUGTRAQ MILWORM SECUNIA OSVDB
availscript -- jobs_portal_script	Unrestricted file upload vulnerability in editlogo.php in AvailScript Jobs Portal Script allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as an image or logo, then accessing it via a direct request to the file in an unspecified directory.	2009-08-21	6.5	CVE-2008-7021 XF BID MILWORM SECUNIA
baidu -- baidu_hi_im	NetService.dll in Baidu Hi IM allows remote servers to cause a denial of service (client crash) via a crafted login response that triggers a divide-by-zero error.	2009-08-19	5.0	CVE-2008-7013 BUGTRAQ OSVDB
bitmixsoft -- php-lance	Multiple directory traversal vulnerabilities in BitmixSoft PHP-Lance 1.52 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) language parameter to show.php and (2) in parameter to advanced_search.php.	2009-08-21	5.0	CVE-2009-2923 MILWORM
bzip -- compress-raw-bzip2	Off-by-one error in the bzinflate function in Bzip2.xs in the Compress-Raw-Bzip2 module before 2.018 for Perl allows context-dependent attackers to cause a denial of service (application hang or crash) via a crafted bzip2 compressed stream that triggers a buffer overflow, a related issue to CVE-2009-1391.	2009-08-19	4.3	CVE-2009-1884 CONFIRM GENTOO
ca -- host-based_intrusion_prevention_system	kmxIds.sys before 7.3.1.18 in CA Host-Based Intrusion Prevention System (HIPS) 8.1 allows remote attackers to cause a denial of service (system crash) via a malformed packet.	2009-08-19	5.0	CVE-2009-2740 CONFIRM
cacert -- cacert	Cross-site scripting (XSS) vulnerability in analyse.php in CACert 20080921, and possibly other versions before 20080928, allows remote attackers to inject arbitrary web script or HTML via the CN (CommonName) field in the subject of an X.509 certificate.	2009-08-21	4.3	CVE-2008-7017 XF BID MISC
checkpoint -- zonealarm	Buffer overflow in multiscan.exe in Check Point ZoneAlarm Security Suite 7.0.483.000 and 8.0.020.000 allows local users to execute arbitrary code via a file or directory with a long path. NOTE: some of these details are obtained from third party information.	2009-08-19	6.9	CVE-2008-7009 XF VUPEN SECTRACK BID BUGTRAQ SECUNIA OSVDB
checkpoint -- zonealarm	TrueVector in Check Point ZoneAlarm 8.0.020.000, with vsmon.exe running, allows remote HTTP proxies to cause a denial of service (crash) and disable the HIDS module via a crafted response.	2009-08-21	4.3	CVE-2008-7025 XF BID BUGTRAQ
cisco -- ios_xr	Cisco IOS XR 3.4.0 through 3.8.1 allows remote attackers to cause a denial of service (session reset) via a BGP UPDATE message with an invalid attribute, as demonstrated in the wild on 17 August 2009.	2009-08-19	4.3	CVE-2009-2055 CISCO

datingpro -- matchmaking	Multiple cross-site scripting (XSS) vulnerabilities in PG MatchMaking allow remote attackers to inject arbitrary web script or HTML via the show parameter to (1) browse_ladies.php and (2) browse_men.php, the (3) gender parameter to search.php, and the (4) id parameter to services.php.	2009-08-20	4.3	CVE-2009-2882 BID SECUNIA MISC
dd-wrt -- dd-wrt	Multiple cross-site request forgery (CSRF) vulnerabilities in apply.cgi in DD-WRT 24 sp2 allow remote attackers to hijack the authentication of administrators for requests that (1) execute arbitrary commands via the ping_ip parameter; (2) change the administrative credentials via the http_username and http_passwd parameters; (3) enable remote administration via the remote_management parameter; or (4) configure port forwarding via certain from, to, ip, and pro parameters. NOTE: This issue reportedly exists because of a "weak ... anti-CSRF fix" implemented in 24 sp2.	2009-08-14	6.8	CVE-2008-6975 BUGTRAQ BUGTRAQ BUGTRAQ MILWORM MISC
devalcms -- devalcms	Cross-site scripting (XSS) vulnerability in index.php in devalcms 1.4a allows remote attackers to inject arbitrary web script or HTML via the currentpath parameter.	2009-08-19	4.3	CVE-2008-6982 CONFIRM
digital_extreme -- pariah epic_games -- unreal_tournament groove_games -- warpath human_head_studios -- dead_mans_hand red_mercury -- shadow_ops whiptail_interactive -- postal	The Unreal engine, as used in Unreal Tournament 3 1.3, Unreal Tournament 2003 and 2004, Dead Man's Hand, Pariah, WarPath, Postal2, and Shadow Ops, allows remote authenticated users to cause a denial of service (server exit) via multiple file downloads from the server, which triggers an assertion failure when the Closing flag in UnChan.cpp is set.	2009-08-19	4.0	CVE-2008-7011 BID BUGTRAQ OSVDB FULLDISC
efrontlearning -- efront	Unrestricted file upload vulnerability in filesystem3.class.php in eFront 3.5.1 build 2710 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension as an avatar, then accessing it via a direct request to the file in (1) student/avatars/ or (2) professor/avatars/.	2009-08-21	6.8	CVE-2008-7026 BID CONFIRM
elkagroup -- elkapax_cms	Cross-site scripting (XSS) vulnerability in the Search feature in elka CMS (aka Elkapax) allows remote attackers to inject arbitrary web script or HTML via the q parameter to the default URI.	2009-08-21	4.3	CVE-2009-2930 BUGTRAQ
elvinbts -- elvinbts	Multiple cross-site scripting (XSS) vulnerabilities in Elvin 1.2.2 allow remote attackers to inject arbitrary web script or HTML via the (1) component and (2) priority parameters to buglist.php; and the (3) Username (4) E-mail, (5) Pass, and (6) Confirm pass fields to createaccount.php.	2009-08-21	4.3	CVE-2009-2920 XF MILWORM
epic_games -- unreal_tournament frontlines -- fuel_of_war	Unreal engine 3, as used in Unreal Tournament 3 1.3, Frontlines: Fuel of War 1.1.1, and other products, allows remote attackers to cause a denial of service (server exit) via a packet with a large length value that triggers a memory allocation failure.	2009-08-19	5.0	CVE-2008-7015 XF BID BUGTRAQ OSVDB FULLDISC
ezphotogallery -- ezphotogallery	Multiple cross-site scripting (XSS) vulnerabilities in Easy Photo Gallery (aka Ezphotogallery) 2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) galleryid parameter to gallery.php,	2009-08-19	4.3	CVE-2008-6988 XF BUGTRAQ OSVDB

	and the (2) size or (3) imageid parameters to show.php.			OSVDB MILWORM SECUNIA
fhttpd -- fhttpd	fhttpd 0.4.2 allows remote attackers to cause a denial of service (crash) via an Authorization HTTP header with an invalid character after the Basic value.	2009-08-19	5.0	CVE-2008-7014 XF BID MILWORM
fullrevolution -- aspwebalbum	Cross-site scripting (XSS) vulnerability in album.asp in Full Revolution aspWebAlbum 3.2 allows remote attackers to inject arbitrary web script or HTML via the message parameter in a summary action.	2009-08-19	4.3	CVE-2008-6977 XF BID MILWORM MILWORM SECUNIA
fullrevolution -- aspwebalbum	Unrestricted file upload vulnerability in Full Revolution aspWebAlbum 3.2 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in pics/, related to the uploadmedia action in album.asp.	2009-08-19	6.8	CVE-2008-6978 XF BID MILWORM MILWORM SECUNIA OSVDB
garagesalesjunkie -- garagesales_script	Cross-site scripting (XSS) vulnerability in visitor/view.php in GarageSales Script allows remote attackers to inject arbitrary web script or HTML via the key parameter. NOTE: some of these details are obtained from third party information.	2009-08-14	4.3	CVE-2009-2778 XF VUPEN MILWORM SECUNIA
gelatocms -- gelatocms	Cross-site scripting (XSS) vulnerability in admin/comments.php in Gelato CMS 0.95 allows remote attackers to inject arbitrary web script or HTML via the content parameter in a comment. NOTE: some of these details are obtained from third party information.	2009-08-24	4.3	CVE-2008-7039 XF BID MISC OSVDB
google -- chrome	Integer underflow in net/base/escape.cc in chrome.dll in Google Chrome 0.2.149.27 allows remote attackers to cause a denial of service (browser crash) via a URI with an invalid handler followed by a "%" (percent) character, which triggers a buffer over-read, as demonstrated using an "about:%" URI.	2009-08-19	4.3	CVE-2008-6995 XF
google -- chrome	Google Chrome BETA (0.2.149.27) does not prompt the user before saving an executable file, which makes it easier for remote attackers or malware to cause a denial of service (disk consumption) or exploit other vulnerabilities via a URL that references an executable file, possibly related to the "ask where to save each file before downloading" setting.	2009-08-19	5.0	CVE-2008-6996 XF BID BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ OSVDB MILWORM CONFIRM CONFIRM
				CVE-2008-

google -- chrome	Google Chrome 0.2.149.27 allows user-assisted remote attackers to cause a denial of service (browser crash) via an IMG tag with a long src attribute, which triggers the crash when the victim performs an "Inspect Element" action.	2009-08-19	4.3	6997 XF BID MILWoRM OSVDB MISC
hp -- insight_control_suite_for_linux	Cross-site request forgery (CSRF) vulnerability in HP Insight Control Suite For Linux (aka ICE-LX) before 2.11 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-08-14	6.8	CVE-2009-2677 HP HP
hyperstop -- web_host_directory	HyperStop Web Host Directory 1.2 allows remote attackers to bypass authentication and download a database backup via a direct request to admin/backup/db.	2009-08-19	5.0	CVE-2008-7008 XF BID SECUNIA MISC OSVDB
ibm -- db2	Memory leak in the Security component in IBM DB2 8.1 before FP18 on Unix platforms allows attackers to cause a denial of service (memory consumption) via unspecified vectors, related to private memory within the DB2 memory structure.	2009-08-19	5.0	CVE-2009-2858 CONFIRM
ibm -- db2	IBM DB2 8.1 before FP18 allows attackers to obtain unspecified access via a das command.	2009-08-19	4.6	CVE-2009-2859 VUPEN CONFIRM
ibm -- db2	Unspecified vulnerability in db2jds in IBM DB2 8.1 before FP18 allows remote attackers to cause a denial of service (service crash) via "malicious packets."	2009-08-19	5.0	CVE-2009-2860 VUPEN CONFIRM
linux -- kernel linux -- kernel	The load_flat_shared_library function in fs/binfmt_flat.c in the flat subsystem in the Linux kernel before 2.6.31-rc6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by executing a shared flat binary, which triggers an access of an "uninitialized cred pointer."	2009-08-14	4.9	CVE-2009-2768 MLIST CONFIRM MLIST
linux -- kernel linux -- kernel	The do_sigaltstack function in kernel/signal.c in Linux kernel 2.6 before 2.6.31-rc5, when running on 64-bit systems, does not clear certain padding bytes from a structure, which allows local users to obtain sensitive information from the kernel stack via the sigaltstack function.	2009-08-18	4.9	CVE-2009-2847 CONFIRM MLIST MLIST
linux -- kernel	The execve function in the Linux kernel, possibly 2.6.30-rc6 and earlier, does not properly clear the current->clear_child_tid pointer, which allows local users to cause a denial of service (memory corruption) via a clone system call with CLONE_CHILD_SETTID or CLONE_CHILD_CLEARTID enabled, which is not properly handled during thread creation and exit.	2009-08-18	4.7	CVE-2009-2848 MLIST MLIST MLIST
linux -- kernel	The md driver (drivers/md/md.c) in the Linux kernel before 2.6.30.2 might allow local users to cause a denial of service (NULL pointer dereference) via vectors related to "suspend_* sysfs attributes" and the (1) suspend_lo_store or (2) suspend_hi_store	2009-08-18	4.7	CVE-2009-2849 MISC MLIST MLIST

	functions. NOTE: this is only a vulnerability when sysfs is writable by an attacker.			CONFIRM CONFIRM
luke_mewburn -- tnftpd	tnftpd before 20080929 splits large command strings into multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks via unknown vectors, probably involving a crafted ftp:// link to a tnftpd server.	2009-08-21	6.8	CVE-2008-7016 XF SECUNIA OSVDB CONFIRM
microtik -- routeros	MicroTik RouterOS 3.x through 3.13 and 2.x through 2.9.51 allows remote attackers to modify Network Management System (NMS) settings via a crafted SNMP set request.	2009-08-19	6.4	CVE-2008-6976 XF BID MILWORM
nashtech -- easy_php_calendar	Cross-site scripting (XSS) vulnerability in NashTech Easy PHP Calendar 6.3.25 allows remote attackers to inject arbitrary web script or HTML via the Details field (descr parameter) in an Add New Event action in an unspecified request as generated by an add action in index.php.	2009-08-21	4.3	CVE-2008-7018 XF BID BUGTRAQ
natterchat -- natterchat	Multiple cross-site scripting (XSS) vulnerabilities in NatterChat 1.12 allow remote attackers to inject arbitrary web script or HTML via the (1) txtUsername parameter to registerDo.asp, as invoked from register.asp, or (2) txtRoomName parameter to room_new.asp. NOTE: these issues might be resultant from XSS in SQL error messages.	2009-08-24	4.3	CVE-2008-7048 XF OSVDB FULLDISC
neon -- neon	neon before 0.28.6, when expat is used, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.	2009-08-21	4.3	CVE-2009-2473 FEDORA FEDORA SECUNIA MLIST MLIST
neon -- neon	neon before 0.28.6, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-08-21	6.8	CVE-2009-2474 FEDORA FEDORA SECUNIA MLIST MLIST
ntop -- ntop	The checkHTTPpassword function in http.c in ntop 3.3.10 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an Authorization HTTP header that lacks a : (colon) character in the base64-decoded string.	2009-08-21	5.0	CVE-2009-2732 VUPEN BUGTRAQ BUGTRAQ SECUNIA
parallels -- plesk	Plesk 8.6.0, when short mail login names (SHORTNAMES) are enabled, allows remote attackers to bypass authentication and send spam e-mail via a message with (1) a base64-encoded username that begins with a valid shortname, or (2) a username that matches a valid password, as demonstrated using (a) SMTP and qmail, and (b) Courier IMAP and POP3.	2009-08-19	5.8	CVE-2008-6984 XF SECTRACK BID BUGTRAQ OSVDB
	Cross-site scripting (XSS) vulnerability in as_archives.php in phpAdultSite CMS, possibly 2.3.2, allows remote attackers to inject arbitrary web script			CVE-2008-6979 XF

phpadultsite -- phpadultsite_cms	or HTML via the results_per_page parameter to index.php. NOTE: some of these details are obtained from third party information. NOTE: this issue might be resultant from a separate SQL injection vulnerability.	2009-08-19	4.3	BID BUGTRAQ MISC SECUNIA OSVDB
phpadultsite -- phpadultsite_cms	index.php in phpAdultSite CMS, possibly 2.3.2, allows remote attackers to obtain the full installation path via an invalid results_per_page parameter, which leaks the path in an error message. NOTE: this issue might be resultant from a separate SQL injection vulnerability.	2009-08-19	5.0	CVE-2008-6981 XF BUGTRAQ MISC
phpauction -- phpauction	phpAuction 3.2, and possibly 3.3.0 GPL Basic edition, allows remote attackers to obtain configuration information via a direct request to phpinfo.php, which calls the phpinfo function.	2009-08-19	5.0	CVE-2008-6999 XF SECUNIA MISC OSVDB
phpscriptsnow -- world's_tallest_buildings	Cross-site scripting (XSS) vulnerability in bios.php in PHP Scripts Now World's Tallest Buildings allows remote attackers to inject arbitrary web script or HTML via the rank parameter.	2009-08-20	4.3	CVE-2009-2884 XF OSVDB SECUNIA MISC
phpscriptsnow -- president_bios	Cross-site scripting (XSS) vulnerability in bios.php in PHP Scripts Now President Bios allows remote attackers to inject arbitrary web script or HTML via the rank parameter.	2009-08-20	4.3	CVE-2009-2887 XF SECUNIA MISC
phpscriptsnow -- hangman	Cross-site scripting (XSS) vulnerability in index.php in PHP Scripts Now Hangman allows remote attackers to inject arbitrary web script or HTML via the letters parameter.	2009-08-20	4.3	CVE-2009-2889 XF OSVDB SECUNIA MISC
phpscriptsnow -- riddles	Cross-site scripting (XSS) vulnerability in results.php in PHP Scripts Now Riddles allows remote attackers to inject arbitrary web script or HTML via the searchquery parameter.	2009-08-20	4.3	CVE-2009-2890 XF OSVDB SECUNIA MISC
phpversion -- php_vx_guestbook	Free PHP VX Guestbook 1.06 allows remote attackers to bypass authentication and download a backup of the database via a direct request to admin/backupdb.php.	2009-08-19	5.0	CVE-2008-7006 XF
reputation -- reputation	Directory traversal vulnerability in include/reputation/rep_profile.php in the Reputation plugin 2.2.4, 2.2.3, 2.0.4, and earlier for PunBB, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the pun_user[language] parameter.	2009-08-17	6.8	CVE-2009-2787 XF MILWORM SECUNIA MISC OSVDB
ryan.mcgeary -- wp-syntax	WP-Syntax plugin 0.9.1 and earlier for Wordpress, with register_globals enabled, allows remote attackers to execute arbitrary PHP code via the test_filter[wp_head] array parameter to test/index.php, which is used in a call to the	2009-08-18	6.8	CVE-2009-2852 XF BID MTI TAWD M

	call_user_func_array function.			MILWORM
sap -- netweaver	Cross-site scripting (XSS) vulnerability in uddiclient/process in the UDDI client in SAP NetWeaver Application Server (Java) 7.0 allows remote attackers to inject arbitrary web script or HTML via the TModel Key field.	2009-08-21	4.3	CVE-2009-2932 MISC XF SECTRACK BID BUGTRAQ MISC SECUNIA OSVDB
simple_machines -- phpraider	Cross-site scripting (XSS) vulnerability in an unspecified component in Simple Machines phpRaider 1.0.7 allows remote attackers to inject arbitrary web script or HTML via the resistance field. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-24	4.3	CVE-2008-7035 XF BID
squid-cache -- squid	The strListGetItem function in src/HttpHeaderTools.c in Squid 2.7 allows remote attackers to cause a denial of service via a crafted auth header with certain comma delimiters that trigger an infinite loop of calls to the strcspn function.	2009-08-18	5.0	CVE-2009-2855 MISC MLIST MLIST MLIST MISC CONFIRM
sun -- opensolaris sun -- solaris	The kernel in Sun Solaris 8, 9, and 10, and OpenSolaris before snv_103, does not properly handle interaction between the filesystem and virtual-memory implementations, which allows local users to cause a denial of service (deadlock and system halt) via vectors involving mmap and write operations on the same file.	2009-08-19	4.9	CVE-2009-2857 SUNALERT CONFIRM
sun -- opensolaris sun -- solaris	The (1) sendfile and (2) sendfilev functions in Sun Solaris 8 through 10, and OpenSolaris before snv_110, allow local users to cause a denial of service (panic) via vectors related to vnode function calls.	2009-08-21	4.9	CVE-2009-2912 SUNALERT CONFIRM
tgs-cms -- tgs_content_management	Cross-site scripting (XSS) vulnerability in login.php in TGS Content Management 0.x allows remote attackers to inject arbitrary web script or HTML via the previous_page parameter, a different vector than CVE-2008-6839.	2009-08-21	4.3	CVE-2009-2928 XF MILWORM
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in the administrator interface in WordPress before 2.8.2 allows remote attackers to inject arbitrary web script or HTML via a comment author URL.	2009-08-18	4.3	CVE-2009-2851 CONFIRM
wordpress -- wordpress	Wordpress before 2.8.3 does not check capabilities for certain actions, which allows remote attackers to make unauthorized edits or additions via a direct request to (1) edit-comments.php, (2) edit-pages.php, (3) edit.php, (4) edit-category-form.php, (5) edit-link-category-form.php, (6) edit-tag-form.php, (7) export.php, (8) import.php, or (9) link-add.php in wp-admin/.	2009-08-18	6.4	CVE-2009-2854 CONFIRM
xzeroscripts	Multiple cross-site scripting (XSS) vulnerabilities in index.php in XZero Community Classifieds 4.97.8	2009-08		CVE-2009-2893 VTDEN

xzeroscripts -- xzero_community_classifieds	allow remote attackers to inject arbitrary web script or HTML via (1) the postevent parameter in a post action or (2) the _xzcal_y parameter.	2009-08-20	4.3	VUPEN BID SECUNIA MISC
xzeroscripts -- xzero_community_classifieds	Cross-site scripting (XSS) vulnerability in index.php in XZero Community Classifieds 4.97.8 allows remote attackers to inject arbitrary web script or HTML via the URI. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-21	4.3	CVE-2009-2913 SECUNIA
xzeroscripts -- xzero_community_classifieds	Cross-site scripting (XSS) vulnerability in index.php in XZero Community Classifieds 4.97.8 and earlier allows remote attackers to inject arbitrary web script or HTML via the name of an uploaded file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-21	4.3	CVE-2009-2914 VUPEN
zen-cart -- zen_cart zen_cart -- zen_cart	Multiple SQL injection vulnerabilities in includes/classes/shopping_cart.php in Zen Cart 1.2.0 through 1.3.8a, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the id parameter when (1) adding or (2) updating the shopping cart.	2009-08-19	6.8	CVE-2008-6985 CONFIRM BID BUGTRAQ BUGTRAQ OSVDB MISC SECUNIA
zen-cart -- zen_cart	SQL injection vulnerability in the actionMultipleAddProduct function in includes/classes/shopping_cart.php in Zen Cart 1.3.0 through 1.3.8a, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the products_id array parameter in a multiple_products_add_product action, a different vulnerability than CVE-2008-6985.	2009-08-19	6.8	CVE-2008-6986 CONFIRM BID BUGTRAQ BUGTRAQ OSVDB MISC SECUNIA

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flex	Cross-site scripting (XSS) vulnerability in index.template.html in the express-install templates in the SDK in Adobe Flex before 3.4, when the installed Flash version is older than a specified requiredMajorVersion value, allows remote attackers to inject arbitrary web script or HTML via the query string.	2009-08-21	2.6	CVE-2009-1879 CONFIRM
boonex -- orca	Cross-site scripting (XSS) vulnerability in Boonex Orca 2.0 and 2.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the topic title field.	2009-08-21	3.5	CVE-2009-2919 XF BID MISC
ca -- internet_security_suite	vetmonnt.sys in CA Internet Security Suite r3, vetmonnt.sys before 9.0.0.184 in Internet Security Suite r4, and vetmonnt.sys before 10.0.0.217 in Internet Security Suite r5 do not properly verify IOCTL calls, which allows local users to cause a denial of service (system crash) via a crafted call.	2009-08-19	2.1	CVE-2009-0682 CONFIRM BUGTRAQ

cisco -- ios_xr	Cisco IOS XR 3.8.1 and earlier allows remote attackers to cause a denial of service (process crash) via a long BGP UPDATE message, as demonstrated by a message with many AS numbers in the AS Path Attribute.	2009-08-21	3.3	CVE-2009-1154 CISCO
cisco -- ios_xr	Cisco IOS XR 3.8.1 and earlier allows remote authenticated users to cause a denial of service (process crash) via vectors involving a BGP UPDATE message with many AS numbers prepended to the AS path.	2009-08-21	3.3	CVE-2009-2056 CISCO
mcafee -- safeboot_device_encryption	McAfee SafeBoot Device Encryption 4 build 4750 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	2009-08-21	2.1	CVE-2008-7020 XF MISC MISC SECUNIA FULLDISC
sun -- virtual_desktop_infrastructure	Sun Virtual Desktop Infrastructure (VDI) 3.0, when anonymous binding is enabled, does not properly handle a client's attempt to establish an authenticated and encrypted connection, which might allow remote attackers to read cleartext VDI configuration-data requests by sniffing LDAP sessions on the network.	2009-08-18	3.5	CVE-2009-2856 VUPEN SUNALERT CONFIRM
thegreenbow -- thegreenbow_vpn_client	The tgbvpn.sys driver in TheGreenBow IPSec VPN Client 4.61.003 allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted request to the 0x80000034 IOCTL, probably involving an input or output buffer size of 0.	2009-08-21	2.1	CVE-2009-2918 MISC VUPEN BUGTRAQ SECUNIA

[Back to top](#)

Last updated August 24, 2009

 Print This Document